PAUL ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC., a Delaware Corporation, Plaintiff, v. CISCO SYSTEMS, INC., a California Corporation, Defendant.	Case No.: **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. ("Finjan") files this Complaint for Patent Infringement and Demand for Jury Trial against Cisco Systems, Inc. ("Defendant" or "Cisco") and allege as follows:

THE PARTIES

1. Finjan is a Delaware Corporation, with its principal place of business at 2000 University Avenue, Suite 600, E. Palo Alto, California 94303.

2. Cisco is a California Corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco may be served through its agent for service of process CSC at 2710 Gateway Oaks Dr. Ste. 150N, Sacramento, California 95833.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

4. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant does business in this District and have, and continues to, infringe and/or induce the infringement in this District. In addition, the Court has personal jurisdiction over Defendant because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-wide basis.

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats recognized today under the umbrella of "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of

content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous patents covering innovations in the United States and around the world resulting directly from Finjan's more than decades-long research and development efforts, supported by a dozen inventors, and over $65 million in R&D investments.

8. Finjan built and sold software, including application program interfaces (APIs), and appliances for network security using these patented technologies. These products and related customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed nearly 150 employees around the world building and selling security products and operating the Malicious Code Research Center through which it frequently published research regarding network security and current threats on the Internet. Finjan's pioneering approach to online security drew equity investments from two major software and technology companies, the first in 2005, followed by the second in 2006. Finjan generated millions of dollars in product sales and related services and support revenues through 2009 when it spun off certain hardware and technology assets in a merger. Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under which it could not make or sell a competing product or disclose the existence of the non-compete clause. Finjan became a publicly traded company in June 2013, capitalized with $30 million. After Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, Finjan re-entered the development and production sector of secure mobile products for the consumer market.

9. Finjan and Cisco's relationship dates back to the early 2000's when Cisco invested in Finjan, seeing the value of Finjan's technology. Throughout the years Cisco and Finjan maintained an amicable relationship and consistently collaborated together on cybersecurity. In the second half of 2013, Cisco acquired the company Sourcefire, Inc. ("SourceFire") and integrated that company's appliances and technology into Cisco's own product lines. It was after this acquisition that Finjan approached Cisco about obtaining a license to Finjan's patents in order cover the technology acquired in the SourceFire deal, along with other unlicensed technologies that Cisco has implemented over the years. Finjan entered into licensing discussions with Cisco under a mutual non-disclosure and

standstill agreement (“Agreement”) dated March 21, 2014, with an expectation that these discussions would be meaningful and productive. To the contrary, Cisco consistently delayed meetings and refused to hold material negotiations. The Agreement for these discussions had been extended five times for a period of over two years, and has now expired.

10. On November 28, 2000, U.S. Patent No. 6,154,844 (“the ‘844 Patent”), titled SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE, was issued to Shlomo Touboul and Nachshon Gal. A true and correct copy of the ‘844 Patent is attached to this Complaint as Exhibit 1 and is incorporated by reference herein.

11. All rights, title, and interest in the ‘844 Patent have been assigned to Finjan, who is the sole owner of the ‘844 Patent. Finjan has been the sole owner of the ‘844 Patent since its issuance.

12. The ‘844 Patent is generally directed towards computer networks, and more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by linking a security profile to such web-based content to facilitate the protection of computers and networks from malicious web-based content.

13. On October 12, 2004, U.S. Patent No. 6,804,780 (“the ‘780 Patent”), titled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. A true and correct copy of the ‘780 Patent is attached to this Complaint as Exhibit 2 and is incorporated by reference herein.

14. All rights, title, and interest in the ‘780 Patent have been assigned to Finjan, who is the sole owner of the ‘780 Patent. Finjan has been the sole owner of the ‘780 Patent since its issuance.

15. The ‘780 Patent is generally directed towards methods and systems for generating a Downloadable ID. By generating an identification for each examined Downloadable, the system may allow for the Downloadable to be recognized without reevaluation. Such recognition increases efficiency while also saving valuable resources, such as memory and computing power.

16. On January 12, 2010, U.S. Patent No. 7,647,633 (“the ‘633 Patent”), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued

to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and correct copy of the ‘633 Patent is attached to this Complaint as Exhibit 3 and is incorporated by reference herein.

17. All rights, title, and interest in the ‘633 Patent have been assigned to Finjan, who is the sole owner of the ‘633 Patent. Finjan has been the sole owner of the ‘633 Patent since its issuance.

18. The ‘633 Patent is generally directed towards computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code.

19. On March 20, 2012, U.S. Patent No. 8,141,154 (“the ‘154 Patent”), titled SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the ‘154 Patent is attached to this Complaint as Exhibit 4 and is incorporated by reference herein.

20. All rights, title, and interest in the ‘154 Patent have been assigned to Finjan, who is the sole owner of the ‘154 Patent. Finjan has been the sole owner of the ‘154 Patent since its issuance.

21. The ‘154 Patent is generally directed towards a gateway computer protecting a client computer from dynamically generated malicious content. One way this is accomplished is to use a content processor to process a first function and invoke a second function if a security computer indicates that it is safe to invoke the second function.

22. On March 18, 2014, U.S. Patent No. 8,677,494 (“the ‘494 Patent”), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and correct copy of the ‘494 Patent is attached to this Complaint as Exhibit 5 and is incorporated by reference herein.

23. All rights, title, and interest in the ‘494 Patent have been assigned to Finjan, who is the sole owner of the ‘494 Patent. Finjan has been the sole owner of the ‘494 Patent since its issuance.

24. The ‘494 Patent is generally directed towards a method and system for deriving security profiles and storing the security profiles. The claims generally cover deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database.

CISCO

25. Cisco makes, uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize Cisco’s Advanced Malware Protection (“AMP”), Cisco Collective Security Intelligence (“CCSI”), Cisco Outbreak Filters, Talos Security Intelligence and Research Group (“Talos”), and AMP Threat Grid technologies, including Cisco AMP for Endpoints, Cisco AMP for Networks (also referred to by Cisco as “NGIPS”), Cisco AMP for ASA with FirePOWER Services, Cisco AMP Private Cloud Virtual Appliance, Cisco AMP for CWS, ESA, or WSA, Cisco AMP for Meraki MX, Cisco AMP Threat Grid (collectively, “Accused AMP Products”). *See* https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/at-a-glance-c45-731876.pdf, attached hereto as Exhibit 6.

26. Cisco AMP for Endpoint products operate on multiple operating systems, including Windows, Mac OS, Linux, and Android, as described in http://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html, attached hereto as Exhibit 7.

27. Cisco AMP for Networks products include AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, and AMP8390, as described in http://www.cisco.com/c/en/us/products/collateral/security/amp-appliances/datasheet-c78-733182.html, attached hereto as Exhibit 8.

28. Cisco AMP for ASA with FirePOWER Services products include Cisco ASA 5506-X, Cisco ASA 5506W-X, Cisco ASA 5506H-X, Cisco ASA 5508-X, Cisco ASA 5516-X, Cisco ASA 5512-X, Cisco ASA 5515-X, Cisco ASA 5525-X, Cisco ASA 5545-X, Cisco ASA 5555-X, Cisco ASA 5585-X SSP-10, Cisco ASA 5585-X SSP-20, Cisco ASA 5585-X SSP-40, Cisco ASA 5585-X SSP-60, Cisco ASA 5585-X SSP EP 10/40, and Cisco ASA 5585-X SSP EP 20/60, as described in

http://cisco-apps.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html, attached hereto as Exhibit 9.

29. Cisco AMP Private Cloud Virtual Appliance products are AMP Private Cloud 2.0, as described in http://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-733180.html, attached hereto as Exhibit 10.

30. Cisco AMP for CWS includes Cloud Web Security Essentials, Cloud Web Security Premium license, Advanced Threat Detection, Cisco AMP license, and Web Security bundle, as described in http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/data_sheet_c78-729637.html, attached hereto as Exhibit 11.

31. Cisco AMP for ESA products include ESA C690, ESA C690X, ESA C680, ESA C390, ESA C380, ESA C190, ESA C170, ESAV C100v, ESAV C300v, ESAV C600v, SMA M690/690X/680, SMA M390/380 and SMA M190/170, as described in http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/data-sheet-c78-729751.html, attached hereto as Exhibit 12.

32. Cisco AMP for WSA products include S690, S690X, S680, S390, S380, S190, S170, S690, WSAV S000v, WSAV S100v, WSAV S300v, M680, M380, and M170, as described in http://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet-c78-729630.html, attached hereto as Exhibit 13.

33. Cisco AMP for Meraki MX is included with Meraki MX products that have the MX Advanced Security License, including MX64, MX64W, MX65, MX65W, MX84, MX100, MX400, MX600, as described in http://blogs.cisco.com/security/cisco-meraki-mx-with-amp-threat-grid, https://meraki.cisco.com/products/appliances#models and https://meraki.cisco.com/amp?utm_source=overview%20features&utm_medium=overview&utm_campaign=AMP%20launch%202016, attached hereto as Exhibits 14-16.

34. Cisco AMP Threat Grid products include Cisco AMP Threat Grid 5000, Cisco AMP Threat Grid 5500, AMP Threat Grid portal, and AMP Threat Grid dynamic analysis, as described in http://www.cisco.com/c/en/us/products/collateral/security/amp-threat-grid-appliances/datasheet-c78-

733667.html and http://www.cisco.com/c/en/us/products/collateral/security/amp-threat-grid-cloud/datasheet-c78-733495.html, attached hereto as Exhibits 17-18.

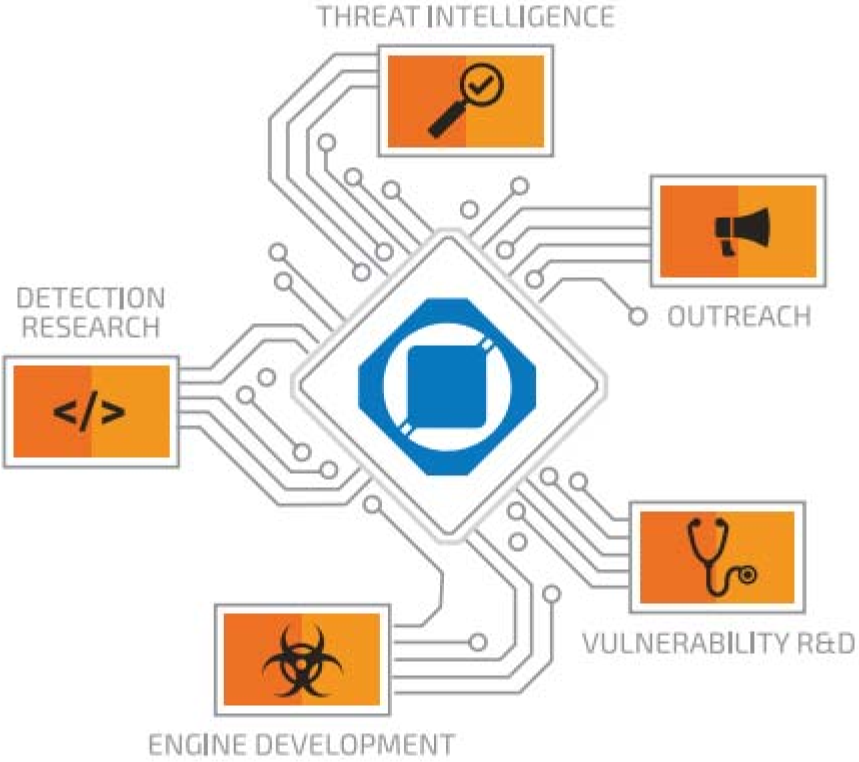
35. In addition, Cisco makes, has made, uses, sells, offers for sale, and/or imports into the United States and this District the Talos service that detects, analyzes and protects against both known and emerging threats, utilizing systems that create threat intelligence for Cisco products (collectively, "Accused Talos Service"), as described in http://blogs.cisco.com/author/talos, attached hereto as Exhibit 19.

36. Further, Cisco makes, has made, uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize Cisco's Outbreak Filters (also known as IronPort Outbreak Filters) with Talos, including Cisco's ESA appliances: ESA C690, ESA C690X, ESA C680, ESA C390, ESA C380, ESA C190, ESA C170, ESAV C100v, ESAV C300v, ESAV C600v, SMA M690/690X/680, SMA M390/380 and SMA M190/170 (collectively, "Accused Outbreak Filter Products"), as described in http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/data-sheet-c78-729751.html, attached hereto as Exhibit 20.

Talos

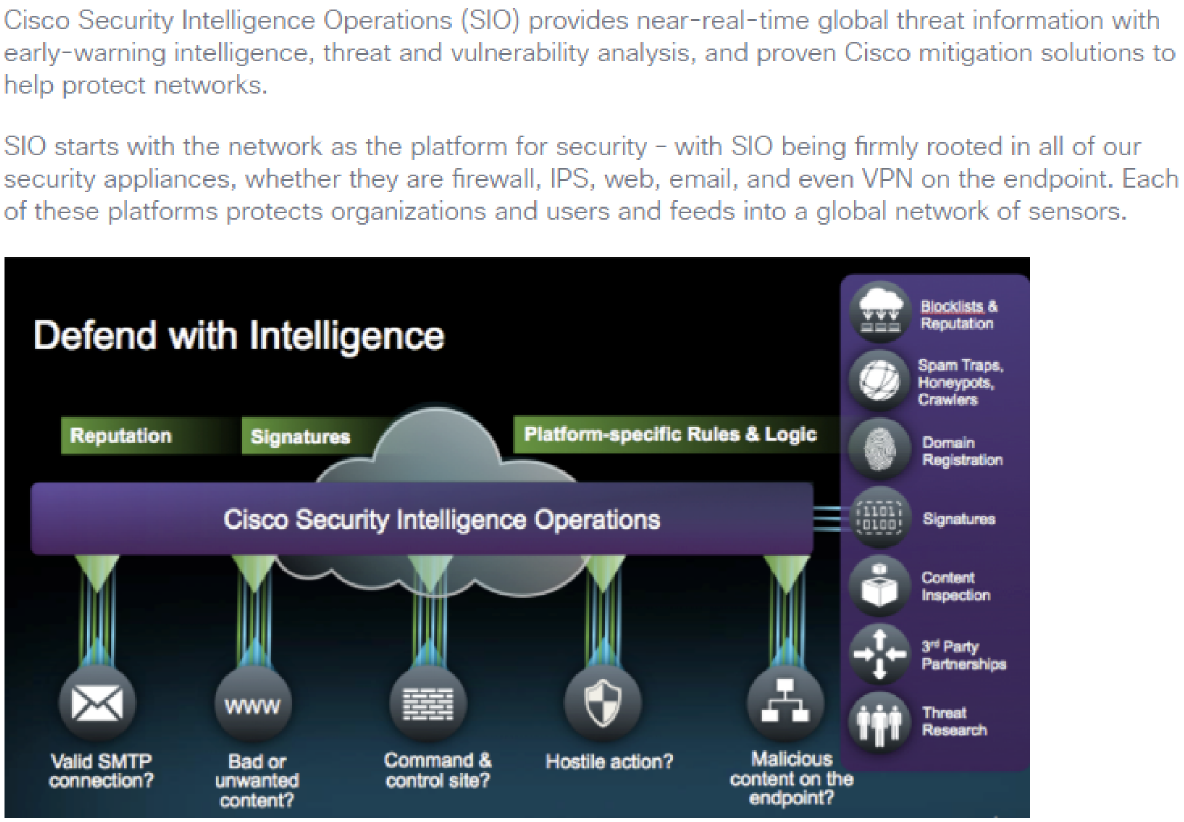
37. Talos Security Intelligence and Research Group ("Talos") was created by combining SourceFire's Vulnerability Research Team, the Cisco Threat Research and Communications group, and the Cisco Security Applications Group. Talos is also a part of the Cisco Security Intelligence Operations ("SIO") and primary member of Cisco's Collective Security Intelligence ecosystem ("CSI"). Talos detects and correlates threats in real time using a threat detection network spanning web, email, malware samples, open source data sets, endpoint intelligence, and network intrusions. Talos encompasses five key areas, including Detection Research, Threat Intelligence, Engine Development, Vulnerability Research and Development, and Outreach. Detection Research consists of vulnerability and malware analyses that lead to the development of detection content for all Cisco's security products. Threat Intelligence consists of correlating and tracking threats in order to turn attribution information into actionable threat intelligence. Engine Development ensures various

inspection engines stay current and maintain their ability to detect and address emerging threats. Vulnerability Research and Development develops ways to identify "Zero-Day" security issues on platforms and operating systems.



See http://www.talosintelligence.com/files/about/Talos_WhitePaper.v3.20160507.pdf, attached hereto as Exhibit 21.

38. SIO is an advanced security infrastructure that provides threat identification, analysis, and mitigation to continuously provide security for Cisco customers. Cisco devices, whether on premise or cloud appliance based, act as the enforcement points in this ecosystem – they use Cisco SIO filters and reputation data to block or allow traffic. The devices also contribute threat intelligence and data back into Cisco SIO. Cisco SIO's dynamic updates deliver current and complete security information to Cisco customers and devices.



Cisco Security Intelligence Operations (SIO) provides near-real-time global threat information with early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks.

SIO starts with the network as the platform for security – with SIO being firmly rooted in all of our security appliances, whether they are firewall, IPS, web, email, and even VPN on the endpoint. Each of these platforms protects organizations and users and feeds into a global network of sensors.

Defend with Intelligence

Reputation

Signatures

Platform-specific Rules & Logic

Cisco Security Intelligence Operations

Valid SMTP connection?

Bad or unwanted content?

Command & control site?

Hostile action?

Malicious content on the endpoint?

Blocklists & Reputation

Spam Traps, Honeypots, Crawlers

Domain Registration

Signatures

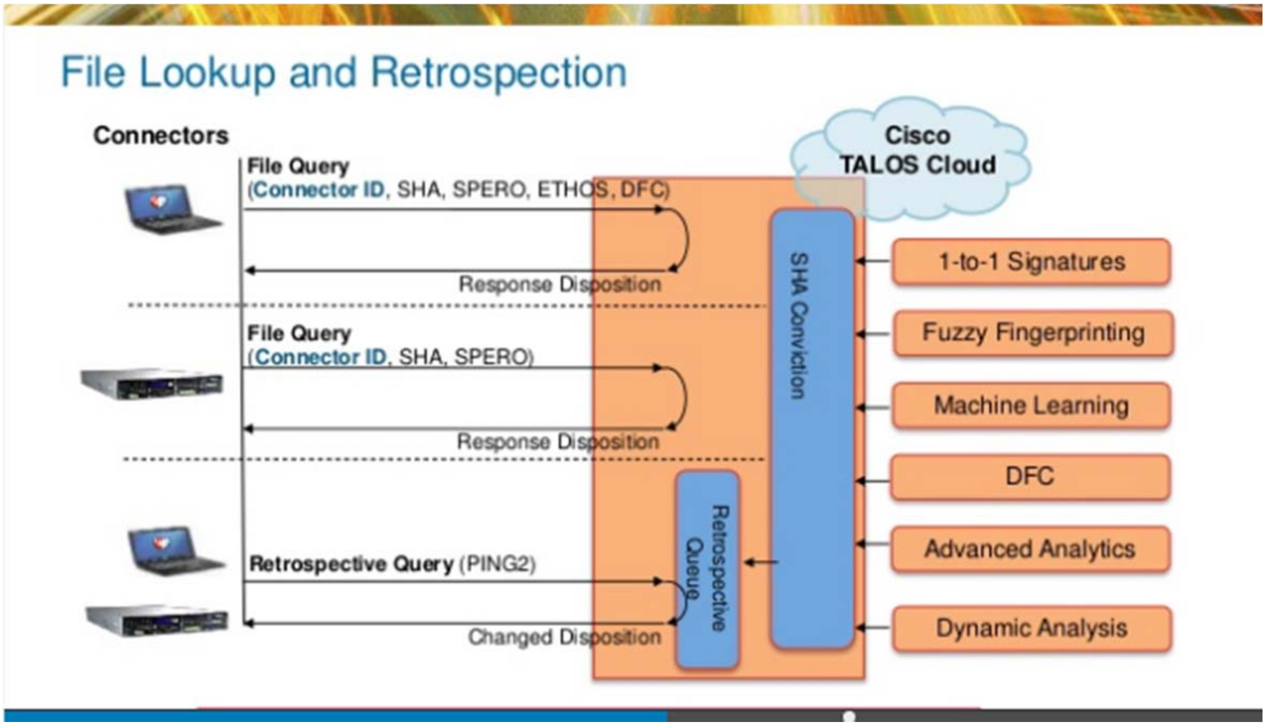
Content Inspection

3rd Party Partnerships

Threat Research

See http://blogs.cisco.com/ciscoit/cisco-security-intelligence-operations-defense-in-depth, attached hereto as Exhibit 22.

39. As shown below, the Talos service includes advanced and dynamic analyses.


File Lookup and Retrospection

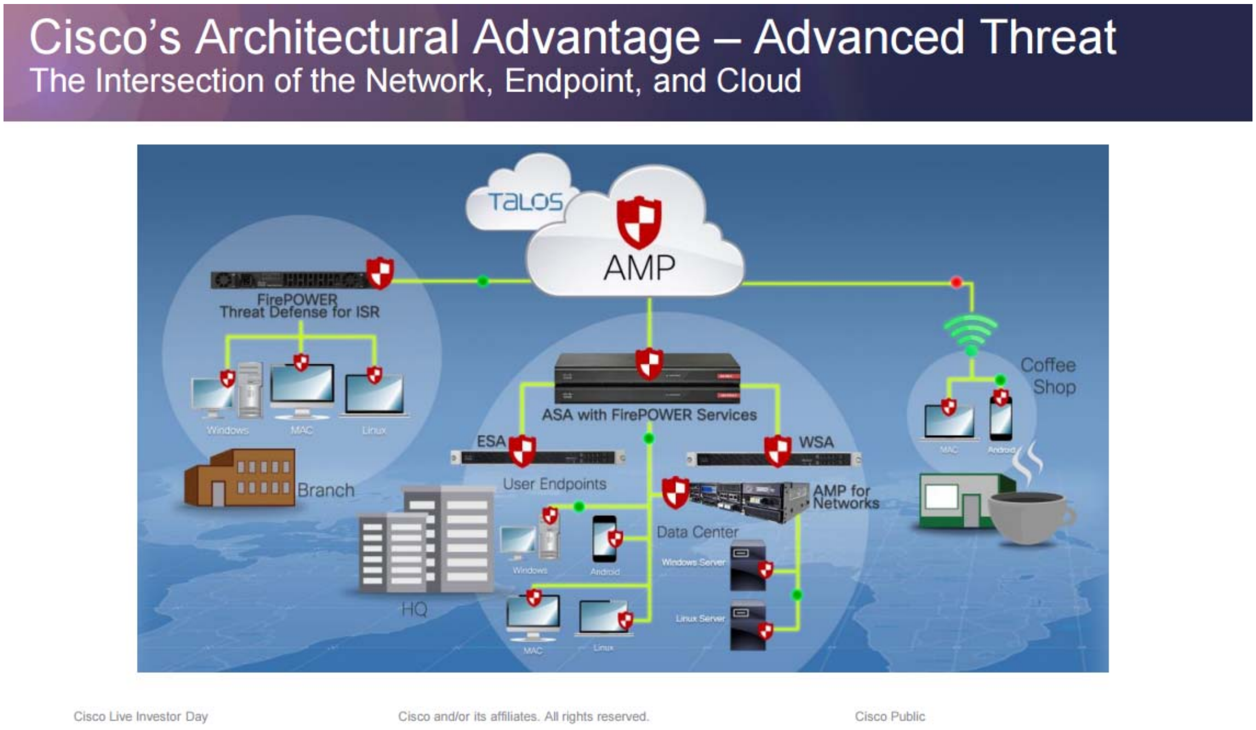
See http://ciscoday.me/pdf/Cisco%20AMP%20Sasa%20Milic%20Asseco.pdf, attached hereto as Exhibit 23.

AMP

40. Cisco AMP uses Cisco's Collective Security Intelligence cloud to obtain real-time file dispositions across multiple attack vectors, like web and email. This includes using Cisco Talos to push threat intelligence to the AMP network. Known malicious files are blocked from reaching their target systems. Files with an unknown dispositions are automatically submitted to the Threat Grid threat intelligence and malware analysis engine for analyses. A threat score is computed for analyzed files and a detailed threat report from Threat Grid is available to aid in decision making. AMP has many variations, including AMP for Endpoints, AMP for Networks, AMP for Firewalls, AMP for ISR, AMP for Web, AMP for E-mail, AMP Private Cloud Virtual Appliance, and Threat Grid.

41. Additionally, the Cisco AMP solution uses an extensive infrastructure of sandboxes to analyze hundreds of thousands of files each day. The Cisco sandboxes detonate files in a safe environment and record its actions. This analysis results in a detained report about the file's disposition (including details regarding major indicators of malicious behavior), potential impact on an

environment, suspicious activity, dynamically linked libraries, indicators of compromise, network activity, and files that may have spawned or dropped.

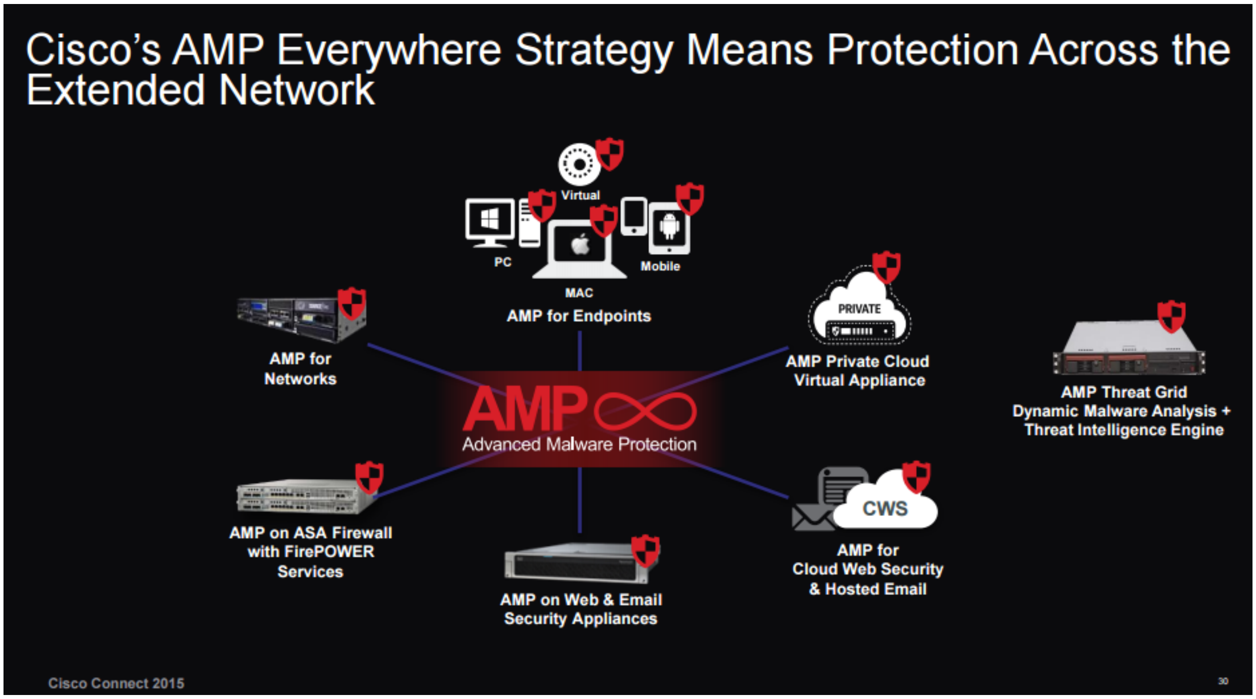


Cisco's Architectural Advantage – Advanced Threat

The Intersection of the Network, Endpoint, and Cloud

Cisco Live Investor Day Cisco and/or its affiliates. All rights reserved. Cisco Public

See http://s2.q4cdn.com/230918913/files/doc_presentations/doc_events/David-Goeckeler_Cisco_Live-Investor_6_8_15_v10_post-legal.pdf, attached hereto as Exhibit 24.



Cisco's AMP Everywhere Strategy Means Protection Across the Extended Network

Virtual

PC

Mobile

MAC

AMP for Endpoints

AMP for Networks

PRIVATE

AMP Private Cloud Virtual Appliance

AMP Threat Grid Dynamic Malware Analysis + Threat Intelligence Engine

AMP Advanced Malware Protection

AMP on ASA Firewall with FirePOWER Services

CWS

AMP for Cloud Web Security & Hosted Email

AMP on Web & Email Security Appliances

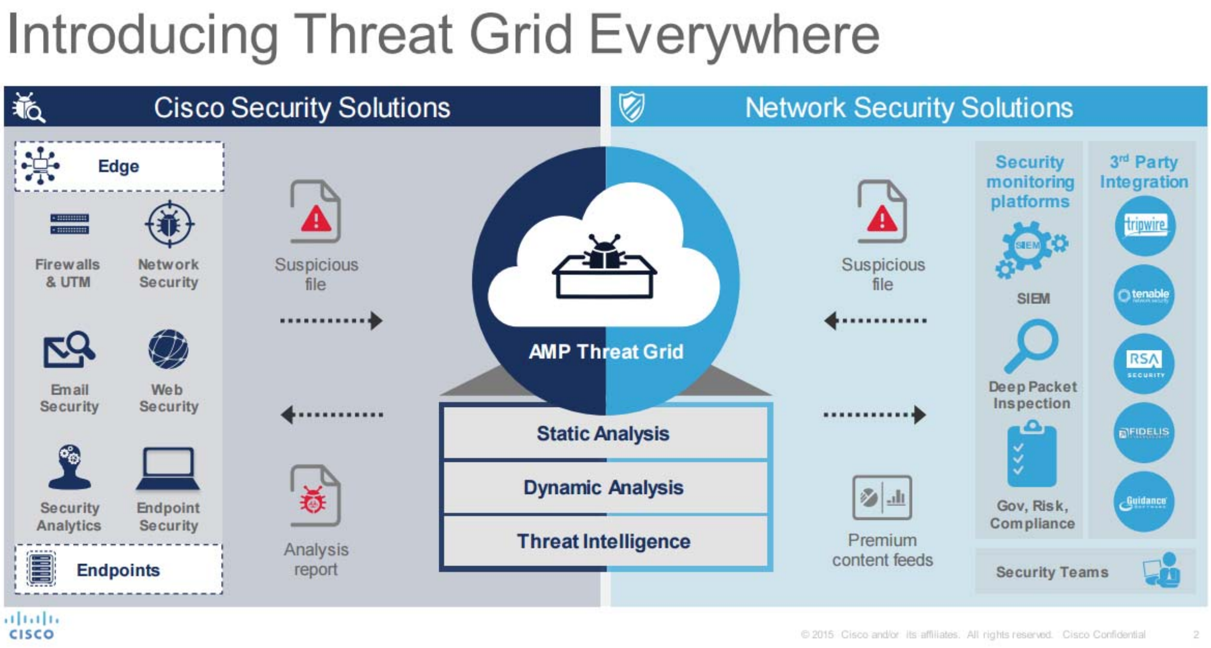
Cisco Connect 2015

30

See https://www.cisco.com/web/offer/emear/38586/images/Presentations/P17.pdf, attached hereto as Exhibit 25.

Threat Grid

42. AMP Threat Grid (both Cloud and Appliance), which crowd sources malware and analyzes all samples using proprietary, utilizes highly secure techniques that include static and dynamic (sandboxing) analysis. AMP Threat Grid analyzes suspicious behavior against more than 450 behavioral indicators. It correlates the results with hundreds of millions of other analyzed malware to provide a global view of malware attacks, campaigns, and their distributions. This ability helps analysts effectively defend against both targeted attacks and the broader threats from advanced malware. AMP Threat Grid's detailed reports include the identification of important behavioral indicators and the assignment of threat scores. Using the behavioral indicators, AMP Threat Grid determines whether a sample is malicious, suspicious, or benign, and why.



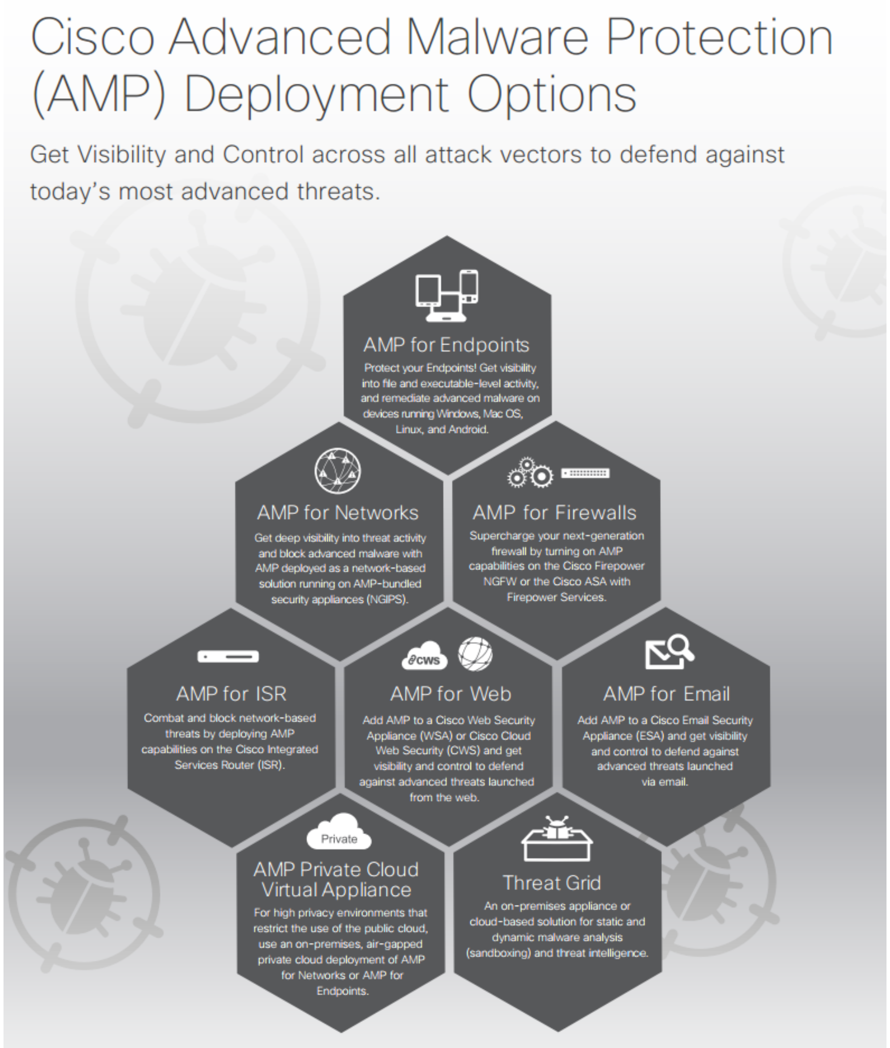
Introducing Threat Grid Everywhere

Cisco Security Solutions

Network Security Solutions

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 2

See http://www.cisco.com/c/dam/global/da_dk/assets/pdfs/AMP-Threat-Grid.pdf, attached hereto as Exhibit 26.



Cisco Advanced Malware Protection (AMP) Deployment Options

Get Visibility and Control across all attack vectors to defend against today's most advanced threats.

AMP for Endpoints

Protect your Endpoints! Get visibility into file and executable-level activity, and remediate advanced malware on devices running Windows, Mac OS, Linux, and Android.

AMP for Networks

Get deep visibility into threat activity and block advanced malware with AMP deployed as a network-based solution running on AMP-bundled security appliances (NGIPS).

AMP for Firewalls

Supercharge your next-generation firewall by turning on AMP capabilities on the Cisco Firepower NGFW or the Cisco ASA with Firepower Services.

AMP for ISR

Combat and block network-based threats by deploying AMP capabilities on the Cisco Integrated Services Router (ISR).

AMP for Web

Add AMP to a Cisco Web Security Appliance (WSA) or Cisco Cloud Web Security (CWS) and get visibility and control to defend against advanced threats launched from the web.

AMP for Email

Add AMP to a Cisco Email Security Appliance (ESA) and get visibility and control to defend against advanced threats launched via email.

AMP Private Cloud Virtual Appliance

For high privacy environments that restrict the use of the public cloud, use an on-premises, air-gapped private cloud deployment of AMP for Networks or AMP for Endpoints.

Threat Grid

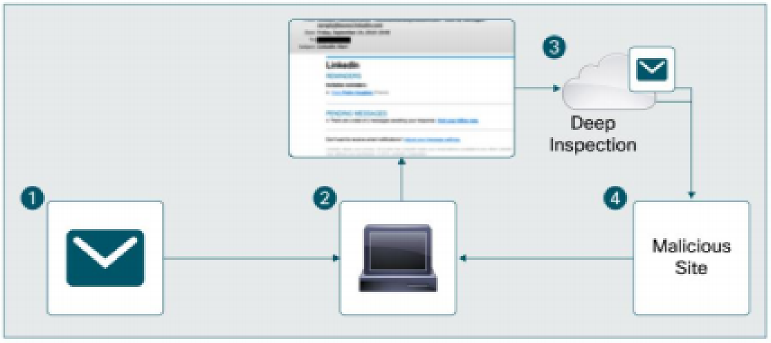
An on-premises appliance or cloud-based solution for static and dynamic malware analysis (sandboxing) and threat intelligence.

See http://www.cisco.com/c/dam/global/en_ca/assets/pdfs/amp-everywhere-deployment-infographic-white.pdf, attached hereto as Exhibit 27.

Outbreak Filters

43. Cisco Outbreak Filters protect systems against new outbreaks of viruses and other malware delivered via attachments by scanning uniform resource locators ("URLs") and processing them in real time—as the user opens them—to block malicious sites. The Cisco Outbreak Filters can also rewrite URLs. Additionally, these filters send data about the websites to Talos to protect all users of Cisco security products, including Cisco's firewall, web security, and intrusion prevention products.

Figure 1. A simple flow of Cisco Outbreak Filters



1. An incoming email is scanned by Outbreak Filters. The refined rule set identifies this as a potential phishing or targeted attack email and handles it as configured on the appliance. By default, a disclaimer is prepended to the email text identifying it as a phish and the URL contained in the email is rewritten.
2. The email with the rewritten url is delivered to the user's inbox.
3. If opened, this rewritten email link sends the user to a public proxy where the webpage content is intercepted and scanned in the cloud in real time using Outbreak Intelligence.
4. If malware is detected on the page, a blocked page message is served up to the user and information about the URL is passed from the cloud back to Cisco Talos. Otherwise, the user is given a choice: surf the page through the proxy or go directly to the site.

See http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white_paper_c11-684611.html at 2, attached hereto as Exhibit 28.

44. Cisco Outbreak Filters use deep content analysis via Outbreak Intelligence processes that look for malicious web content. The content is scanned using multiple proprietary scanning engines for Flash, Java, PDF, archives, executables, file anomalies and more. Additionally, virtual script emulation is used where the script is run within the cloud infrastructure allowing for monitoring of malicious behavior such as a hidden redirect or drive-by download. If malicious behavior is detected, the script is blocked, preventing it from passing onto the end user.

CISCO’S INFRINGEMENT OF FINJAN’S PATENTS

45. Cisco has been and is now infringing, and will continue to infringe the ‘844 Patent, the ‘780 Patent, the ‘633 Patent, the ‘154 Patent, and the ‘494 Patent (collectively “the Patents-In-Suit”) in this judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale the claimed system and methods on the Accused AMP Products, Accused Talos Service, and Accused Outbreak Filter Products.

46. In addition to directly infringing the Patents-In-Suit pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Cisco indirectly infringe all the Patents-In-Suit by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Patents-In-Suit.

COUNT I
(Direct Infringement of the ‘844 Patent pursuant to 35 U.S.C. § 271(a))

47. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

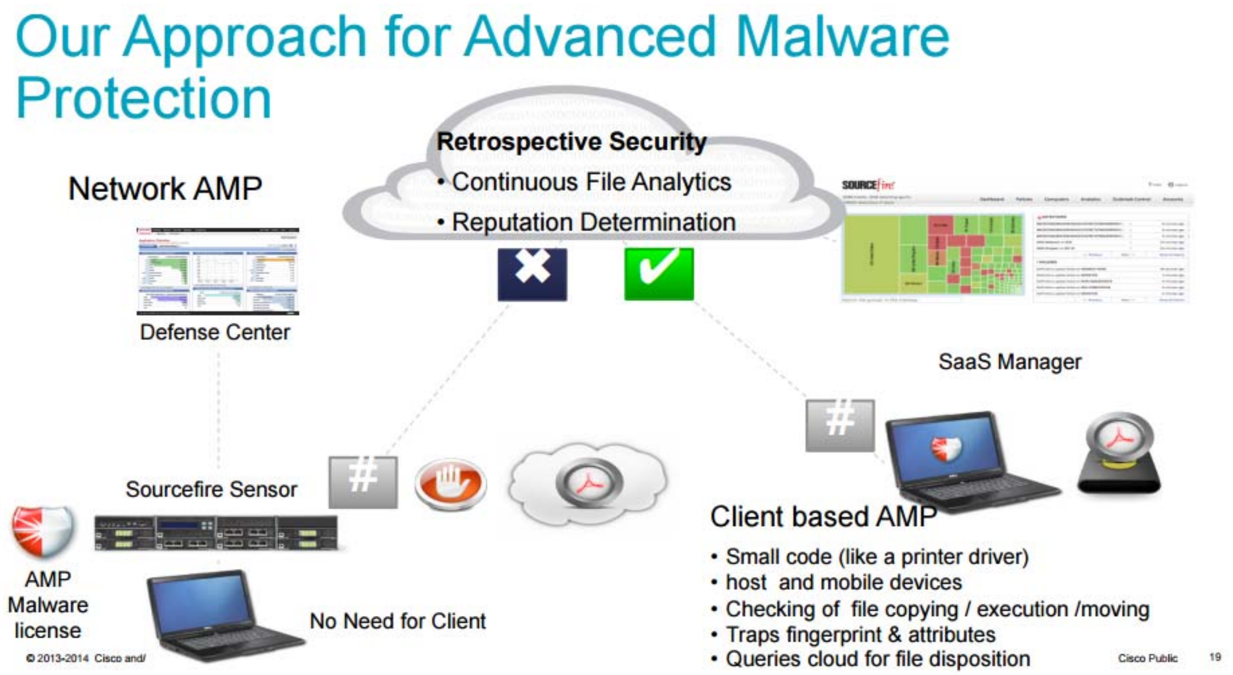
48. Defendant has infringed and continues to infringe Claims 1-44 of the ‘844 Patent in violation of 35 U.S.C. § 271(a).

49. Defendant’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

50. Defendant’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

51. Defendant’s infringement includes the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including the Cisco AMP for Endpoints, Cisco AMP for Networks, Cisco AMP for ASA with FirePOWER Services, Cisco AMP Private Cloud Virtual Appliance, Cisco AMP for CWS, ESA, or WSA, Cisco AMP for Meraki MX, Cisco AMP Threat Grid (i.e., the Accused AMP Products), and the Accused Talos Service (collectively, the “’844 Accused Products”).

52. The ‘844 Accused Products embody the patented invention of the ‘844 Patent and infringe the ‘844 Patent because they practice a method of receiving by an inspector a downloadable, generating by the inspector a first downloadable security profile that identifies suspicious code in the received downloadable and linking by the inspector the first downloadable security profile to the downloadable before a web server makes the downloadable available to web clients. For example, as shown below, Cisco AMP for Networks, provides gateway security to end users.



Our Approach for Advanced Malware Protection

Network AMP

Defense Center

Retrospective Security

- Continuous File Analytics
- Reputation Determination

SaaS Manager

Sourcefire Sensor

AMP Malware license

No Need for Client

Client based AMP

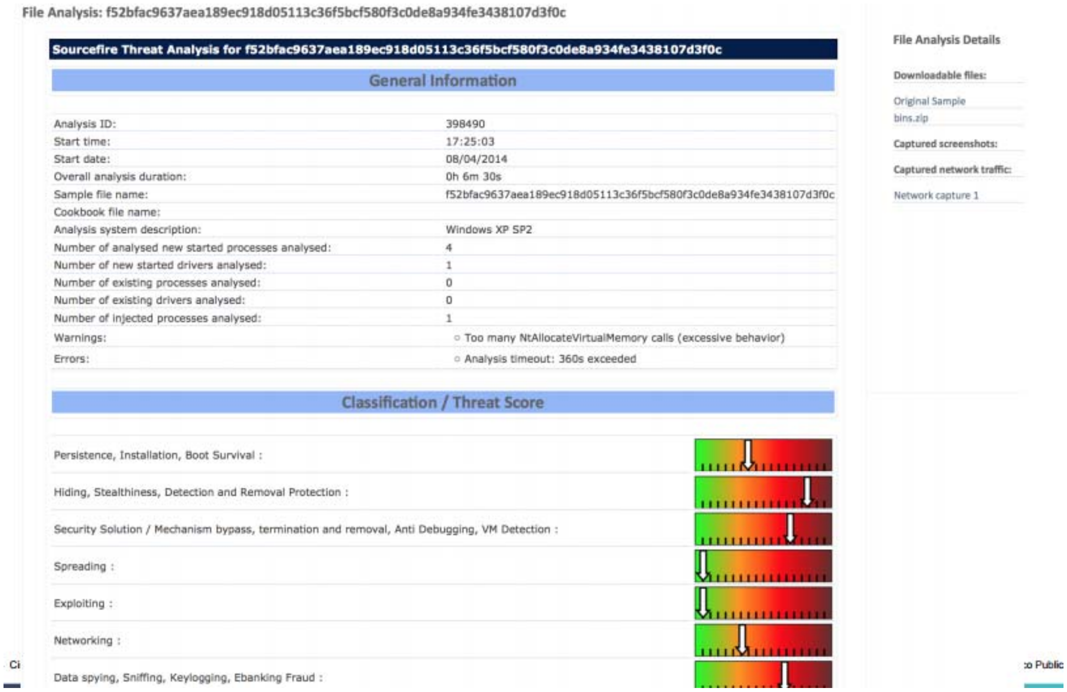
- Small code (like a printer driver)
- host and mobile devices
- Checking of file copying / execution /moving
- Traps fingerprint & attributes
- Queries cloud for file disposition

© 2013-2014 Cisco and/

Cisco Public 19

See http://ftp.cisco.cz/Seminare/2013-ConnectClub/2014-05-28-AMP-GyorgyAcs.pdf, attached hereto as Exhibit 29.

53. Incoming downloadables are received at the ’844 Accused Products, whether the downloadables are either scanned locally or submitted for analytics and reputation determination. As shown below, using advanced heuristics, a downloadable security profile is created and linked if the downloadable is unknown.



File Analysis: f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c

Sourcefire Threat Analysis for f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c

General Information

Analysis ID:	398490
Start time:	17:25:03
Start date:	08/04/2014
Overall analysis duration:	0h 6m 30s
Sample file name:	f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c
Cookbook file name:	
Analysis system description:	Windows XP SP2
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Warnings:	○ Too many NtAllocateVirtualMemory calls (excessive behavior)
Errors:	○ Analysis timeout: 360s exceeded

Classification / Threat Score

Persistence, Installation, Boot Survival :

Hiding, Stealthiness, Detection and Removal Protection :

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection :

Spreading :

Exploiting :

Networking :

Data spying, Sniffing, Keylogging, Ebanking Fraud :

File Analysis Details

Downloadable files:

Original Sample
bins.zip

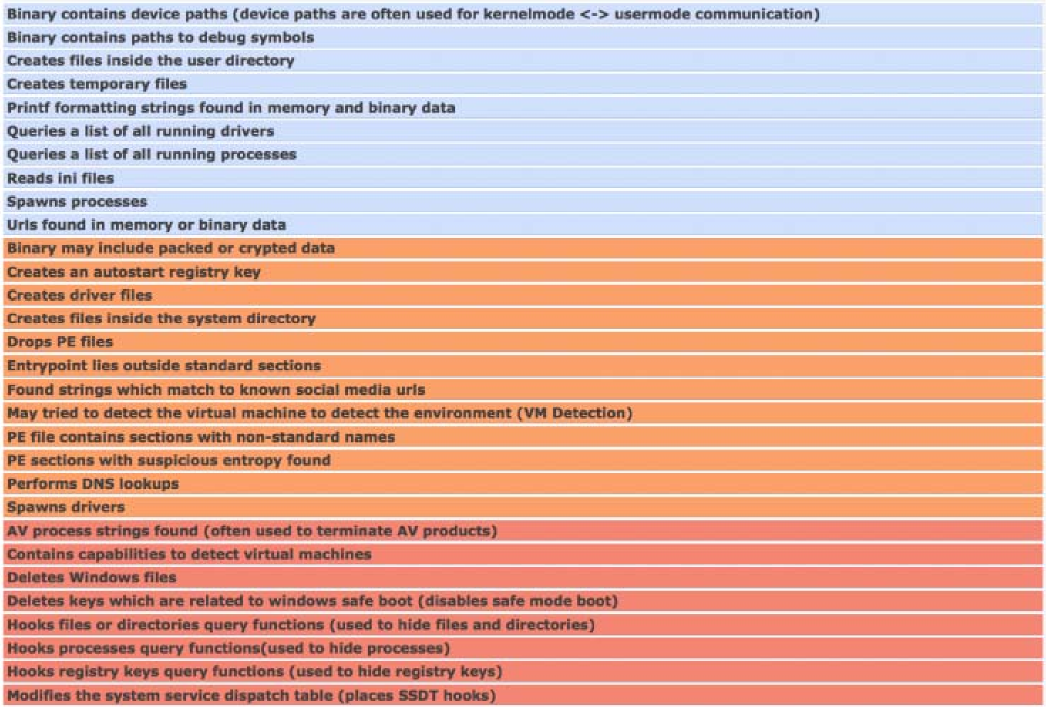
Captured screenshots:

Captured network traffic:

Network capture 1

See http://ftp.cisco.cz/Seminare/2013-ConnectClub/2014-05-28-AMP-GyorgyAcs.pdf, attached hereto as Exhibit 29.

As shown below, a list of suspicious operations is collected.



Binary contains device paths (device paths are often used for kernelmode <-> usermode communication)
Binary contains paths to debug symbols
Creates files inside the user directory
Creates temporary files
Printf formatting strings found in memory and binary data
Queries a list of all running drivers
Queries a list of all running processes
Reads ini files
Spawns processes
Urls found in memory or binary data
Binary may include packed or crypted data
Creates an autostart registry key
Creates driver files
Creates files inside the system directory
Drops PE files
Entrypoint lies outside standard sections
Found strings which match to known social media urls
May tried to detect the virtual machine to detect the environment (VM Detection)
PE file contains sections with non-standard names
PE sections with suspicious entropy found
Performs DNS lookups
Spawns drivers
AV process strings found (often used to terminate AV products)
Contains capabilities to detect virtual machines
Deletes Windows files
Deletes keys which are related to windows safe boot (disables safe mode boot)
Hooks files or directories query functions (used to hide files and directories)
Hooks processes query functions(used to hide processes)
Hooks registry keys query functions (used to hide registry keys)
Modifies the system service dispatch table (places SSDT hooks)

See http://ftp.cisco.cz/Seminare/2013-ConnectClub/2014-05-28-AMP-GyorgyAcs.pdf, attached hereto as Exhibit 29.

54. The Accused AMP Products use the Talos Service and other systems to create a downloadable security profile. Similarly, the Accused Talos Service also generates a downloadable security profile for unknown downloadables.

55. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

56. Defendant's infringement of the '844 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

57. Defendant is well aware of Finjan's patents, including the '844 Patent, and have continued its infringing activity despite this knowledge. Finjan informed Defendant of its patent portfolio and infringement on or about March 2014, and have provided representative claim charts specifically identifying how Defendant's products and services infringe Finjan's patents. Finjan attempted unsuccessfully to actively engage in good faith negotiations for over two years with Defendant regarding Finjan's patent portfolio, including having a number of in-person and telephonic meetings explaining claim element by element of Defendant's infringement.

58. Despite knowledge of Finjan's patent portfolio, being provided representative claim charts of several Finjan patents, including the '844 Patent, and engaging in technical meetings regarding infringement of Defendant's products and services, Defendant has sold and continues to sell the accused products and services in complete disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '844 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II
(Indirect Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(b))

59. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

60. Defendant has induced and continues to induce infringement of one or more claims of the '844 Patent under 35 U.S.C. § 271(b).

61. In addition to directly infringing the '844 Patent, Defendant indirectly infringes the '844 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '844 Patent, where all the steps of the method claims are performed by either Defendant, its customers, purchasers, users or developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '844 Patent, including Claims 1-14 and 23-31.

62. Defendant knowingly and actively aided and abetted the direct infringement of the '844 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '844 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '844 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '844 Patent, specifically through the use of Cisco's AMP, Cisco's CCSI, Talos, and AMP Threat Grid technologies, and by advertising and promoting the use of the '844 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '844 Accused Products in an infringing manner.

63. Defendant updates and maintains an HTTP site with Defendant's quick start guides, administration guides, user guides, and operating instructions which cover in depth aspects of operating Defendant's offerings. *See* http://www.cisco.com/c/en/us/support/index.html/, attached hereto as Exhibit 30; *see also* http://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-

products-support-configure.html, attached hereto as Exhibit 31; http://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-configure.html/, attached hereto as Exhibit 32; http://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html, attached hereto as Exhibit 33; http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/products-configuration-examples-list.html, attached hereto as Exhibit 34; http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-configuration-examples-list.html, attached hereto as Exhibit 35; http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 36; http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 37; https://meraki.cisco.com/support/, attached hereto as Exhibit 38; http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html, attached hereto as Exhibit 39.

COUNT III
(Direct Infringement of the ‘780 Patent pursuant to 35 U.S.C. § 271(a))

64. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

65. Defendant has infringed and continues to infringe Claims 1-18 of the ‘780 Patent in violation of 35 U.S.C. § 271(a).

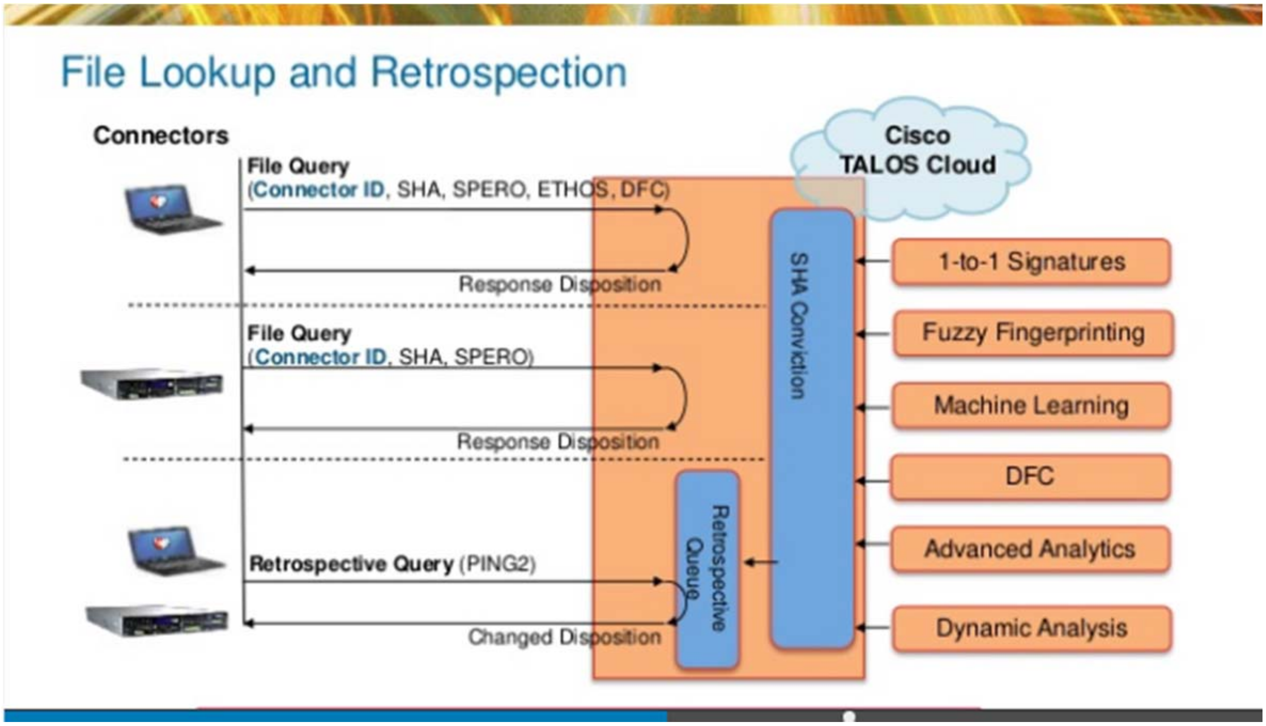
66. Defendant’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

67. Defendant’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

68. Defendant’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including Cisco AMP for Endpoints, Cisco AMP for Networks, Cisco AMP for ASA with FirePOWER Services, Cisco AMP Private Cloud Virtual Appliance, Cisco AMP for CWS, ESA, or WSA, Cisco AMP for Meraki MX,

Cisco AMP Threat Grid (i.e., the Accused AMP Products), and the Accused Talos Service (collectively, the "'780 Accused Products").

69. The '780 Accused Products embody the patented invention of the '780 Patent and infringe the '780 Patent because they practice a method of obtaining a downloadable that includes one or more references to software components required to be executed by the downloadable, fetching at least one software component required to be executed by the downloadable, and performing a hashing function on the downloadable and the fetched software components to generate a Downloadable ID. For example, Cisco AMP for Endpoints perform hash value lookups using SHA256 hashing technology, including dropper files. As shown below, Cisco AMP for Endpoints uses SHA hash to perform lookups in the Talos Cloud.



File Lookup and Retrospection

Connectors

File Query
(Connector ID, SHA, SPERO, ETHOS, DFC)

Response Disposition

File Query
(Connector ID, SHA, SPERO)

Response Disposition

Retrospective Query (PING2)

Changed Disposition

Cisco TALOS Cloud

SHA Conviction

Retrospective Queue

1-to-1 Signatures

Fuzzy Fingerprinting

Machine Learning

DFC

Advanced Analytics

Dynamic Analysis

See http://ciscoday.me/pdf/Cisco%20AMP%20Sasa%20Milic%20Asseco.pdf, attached hereto as Exhibit 23.

In creating that hash value, Cisco AMP for Endpoints obtains the software components required to be executed and performs a hashing function on the downloadable and fetched software components.

70. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

71. Defendant's infringement of the '780 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

72. Defendant is well aware of Finjan's patents, including the '780 Patent, and has continued its infringing activity despite this knowledge. Finjan informed Defendant of its patent portfolio and infringement on or about March 2014, and have provided representative claim charts specifically identifying how Defendant's products and services infringe Finjan's patents. Finjan attempted unsuccessfully to actively engage in good faith negotiations for over two years with Defendant regarding Finjan's patent portfolio, including having a number of in-person and telephonic meetings explaining claim element by element of Defendant's infringement.

73. Despite knowledge of Finjan's patent portfolio, being provided representative claim charts of several Finjan patents and engaging in technical meetings regarding infringement of Defendant's products and services, Defendants has sold and continues to sell the accused products and services in complete disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '780 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT IV
(Indirect Infringement of the '780 Patent pursuant to 35 U.S.C. § 271(b))

74. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

75. Defendant has induced and continues to induce infringement of at least Claims 1-8 of the ‘780 Patent under 35 U.S.C. § 271(b).

76. In addition to directly infringing the ‘780 Patent, Defendant indirectly infringes the ‘780 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘780 Patent, where all the steps of the method claims are performed by either Defendant or its customers, purchasers, users and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the ‘780 Patent, including Claims 1-8.

77. Defendant knowingly and actively aided and abetted the direct infringement of the ‘780 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘780 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the ‘780 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘780 Patent, specifically through the use of Cisco’s AMP, Cisco’s CCSI, Talos, and AMP Threat Grid technologies, and by advertising and promoting the use of the ‘780 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘780 Accused Products in an infringing manner.

78. Defendant updates and maintains an HTTP site with Defendant’s quick start guides, administration guides, user guides, and operating instructions which cover in depth aspects of operating Defendant’s offerings. *See* http://www.cisco.com/c/en/us/support/index.html/, attached hereto as Exhibit 30; *see also* http://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-configure.html, attached hereto as Exhibit 31; http://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-configure.html/, attached hereto as Exhibit 32; http://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html, attached hereto as Exhibit 33;

http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/products-configuration-examples-list.html, attached hereto as Exhibit 34; http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-configuration-examples-list.html, attached hereto as Exhibit 35; http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 36; http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 37; https://meraki.cisco.com/support/, attached hereto as Exhibit 38; http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html, attached hereto as Exhibit 39.

COUNT V
(Direct Infringement of the ‘633 Patent pursuant to 35 U.S.C. § 271(a))

79. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

80. Defendant has infringed and continues to infringe Claims 1-41 of the ‘633 Patent in violation of 35 U.S.C. § 271(a).

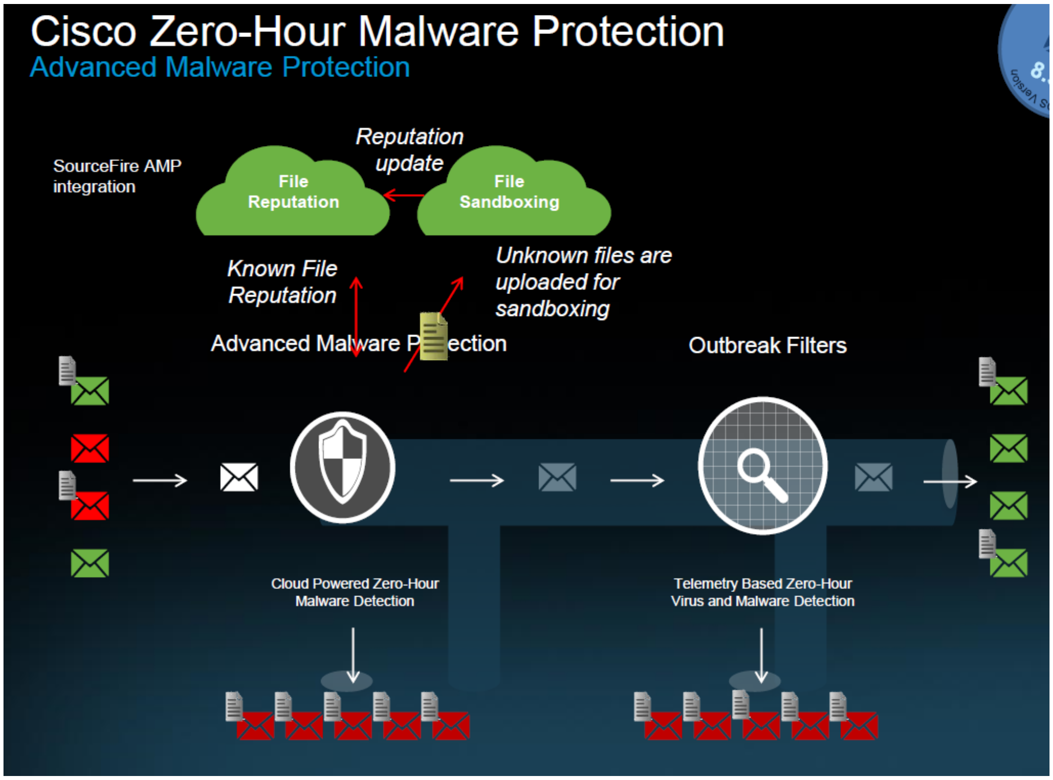
81. Defendant’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

82. Defendant’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

83. Defendant’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including Cisco AMP for Endpoints, Cisco AMP for Networks, Cisco AMP for ASA with FirePOWER Services, Cisco AMP Private Cloud Virtual Appliance, Cisco AMP for CWS, ESA, or WSA, Cisco AMP for Meraki MX, Cisco AMP Threat Grid (i.e., the Accused AMP Products), and the Accused Talos Service (collectively, the “’633 Accused Products”).

84. The ‘633 Accused Products embody the patented invention of the ‘633 Patent and infringe the ‘633 Patent because they practice a method and a system of receiving downloadable

information, determining whether that the downloadable information includes executable code, and transmitting mobile protection code to at least one information destination of the downloadable information if the downloadable information is determined to include executable code. For example, as shown below, the '633 Accused Products provide protection by sending a file for sandboxing with mobile protection code.



Cisco Zero-Hour Malware Protection

Advanced Malware Protection

SourceFire AMP integration
File Reputation
Reputation update
File Sandboxing
Known File Reputation
Unknown files are uploaded for sandboxing
Advanced Malware P ection
Outbreak Filters
Cloud Powered Zero-Hour Malware Detection
Telemetry Based Zero-Hour Virus and Malware Detection

See http://www.cisco.com/assets/global/MK/events/2015/cisco_day/presentations/Gyorgy_Acs-Content_Security_Update.pdf, attached hereto as Exhibit 40.

85. Incoming downloadable information are scanned to determine whether they have executable information. If they include executable information, mobile protection code and the executable code are sent to an information destination, such as a sandbox.

86. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

87. Defendant's infringement of the '633 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

88. Defendant is well aware of Finjan's patents, including the '633 Patent, and has continued its infringing activity despite this knowledge. Finjan informed Defendant of its patent portfolio and infringement on or about March 2014, and have provided representative claim charts specifically identifying how Defendant's products and services infringe Finjan patents. Finjan attempted unsuccessfully to actively engage in good faith negotiations for over two years with Defendant regarding Finjan's patent portfolio, including having a number of in-person and telephonic meetings explaining claim element by element of Defendant's infringement.

89. Despite knowledge of Finjan's patent portfolio, being provided representative claim charts of several Finjan patents, including the '633 Patent, and engaging in technical meetings regarding infringement of Defendant's products and services, Defendant has sold and continues to sell the accused products and services in complete disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '633 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VI
(Indirect Infringement of the '633 Patent pursuant to 35 U.S.C. § 271(b))

90. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

91. Defendant has induced and continues to induce infringement of at least Claims 1-7, 14-20, 28-33, and 42-43 of the '633 Patent under 35 U.S.C. § 271(b).

92. In addition to directly infringing the '633 Patent, Defendant indirectly infringes the '633 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '633 Patent, where all the steps of the method claims are performed by either Defendant, its customers, purchasers, users, and developers, or

some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the ‘633 Patent, including Claims 1-7, 14-20, 28-33, and 42-43.

93. Defendant knowingly and actively aided and abetted the direct infringement of the ‘633 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the ‘633 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the ‘633 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘633 Patent, specifically through the use of Cisco’s AMP, Cisco’s CCSI, Talos, and AMP Threat Grid technologies, and by advertising and promoting the use of the ‘633 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘633 Accused Products in an infringing manner.

94. Defendant updates and maintains an HTTP site with Defendant’s quick start guides, administration guides, user guides, and operating instructions which cover in depth aspects of operating Defendant’s offerings. *See* http://www.cisco.com/c/en/us/support/index.html/, attached hereto as Exhibit 30; *see also* http://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-configure.html, attached hereto as Exhibit 31; http://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-configure.html/, attached hereto as Exhibit 32; http://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html, attached hereto as Exhibit 33; http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/products-configuration-examples-list.html, attached hereto as Exhibit 34; http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-configuration-examples-list.html, attached hereto as Exhibit 35; http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 36; http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 37; https://meraki.cisco.com/support/, attached hereto as Exhibit

38; http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html, attached hereto as Exhibit 39.

COUNT VII
(Direct Infringement of the ‘154 Patent pursuant to 35 U.S.C. § 271(a))

95. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

96. Defendant has infringed and continues to infringe Claims 1-12 of the ‘154 Patent in violation of 35 U.S.C. § 271(a).

97. Defendant’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

98. Defendant’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

99. Defendant’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including Email Security Appliances with Outbreak Filters using the Talos Service, which embody the patented invention of the ‘154 Patent. Such products include ESA C690, ESA C690X, ESA C680, ESA C390, ESA C380, ESA C190, ESA C170, ESAV C100v, ESAV C300v, ESAV C600v, SMA M690/690X/680, SMA M390/380 and SMA M190/170 (collectively, the “’154 Accused Products”).

100. The ‘154 Accused Products embody the patented invention of the ‘154 Patent and infringe the ‘154 Patent because they utilize and/or incorporate a system for protecting a computer from dynamically generated malicious content, comprising a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe; a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input. For example, as

shown below, the '154 Accused Products utilize Outbreak Filters that rewrites incoming emails and provide real-time scanning of links and attachments.

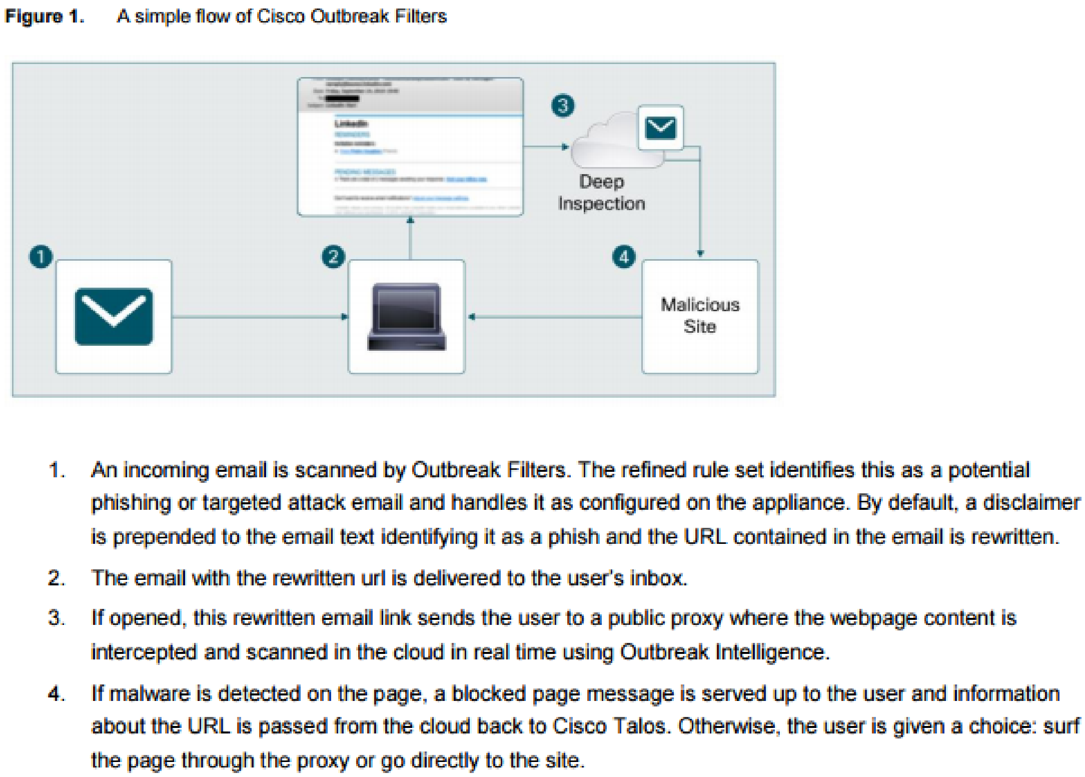


Figure 1. A simple flow of Cisco Outbreak Filters

1. An incoming email is scanned by Outbreak Filters. The refined rule set identifies this as a potential phishing or targeted attack email and handles it as configured on the appliance. By default, a disclaimer is prepended to the email text identifying it as a phish and the URL contained in the email is rewritten.
2. The email with the rewritten url is delivered to the user's inbox.
3. If opened, this rewritten email link sends the user to a public proxy where the webpage content is intercepted and scanned in the cloud in real time using Outbreak Intelligence.
4. If malware is detected on the page, a blocked page message is served up to the user and information about the URL is passed from the cloud back to Cisco Talos. Otherwise, the user is given a choice: surf the page through the proxy or go directly to the site.

See http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white_paper_c11-684611.html at 2, attached hereto as Exhibit 28. Incoming emails are received at the Email Security Appliance, where they are scanned for dynamic content and URL links in the email are rewritten. The rewritten email links redirect to a public proxy were the content is intercepted and scanned in the cloud using Talos and other systems in real time. If the content is safe, the content is sent to the end-user. If the content is malicious, the user is sent blocked page message.

101. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

102. Defendant's infringement of the '154 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

103. Defendant is well aware of Finjan's patents, including the '154 Patent, and has continued its infringing activity despite this knowledge. Finjan informed Defendant of its patent portfolio and infringement on or about March 2014, and have provided representative claim charts specifically identifying how Defendant's products and services infringe Finjan's patents. Finjan attempted unsuccessfully to actively engage in good faith negotiations for over two years with Defendant regarding Finjan's patent portfolio, including having a number of in-person and telephonic meetings explaining claim element by element of Defendant's infringement.

104. Despite knowledge of Finjan's patent portfolio, being provided representative claim charts of several Finjan patents, including the '154 Patent, and engaging in technical meetings regarding infringement of Defendant's products and services, Defendant has sold and continues to sell the accused products and services in complete disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '154 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VIII
(Direct Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(a))

105. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

106. Defendant has infringed and continues to infringe Claims 1-18 of the '494 Patent in violation of 35 U.S.C. § 271(a).

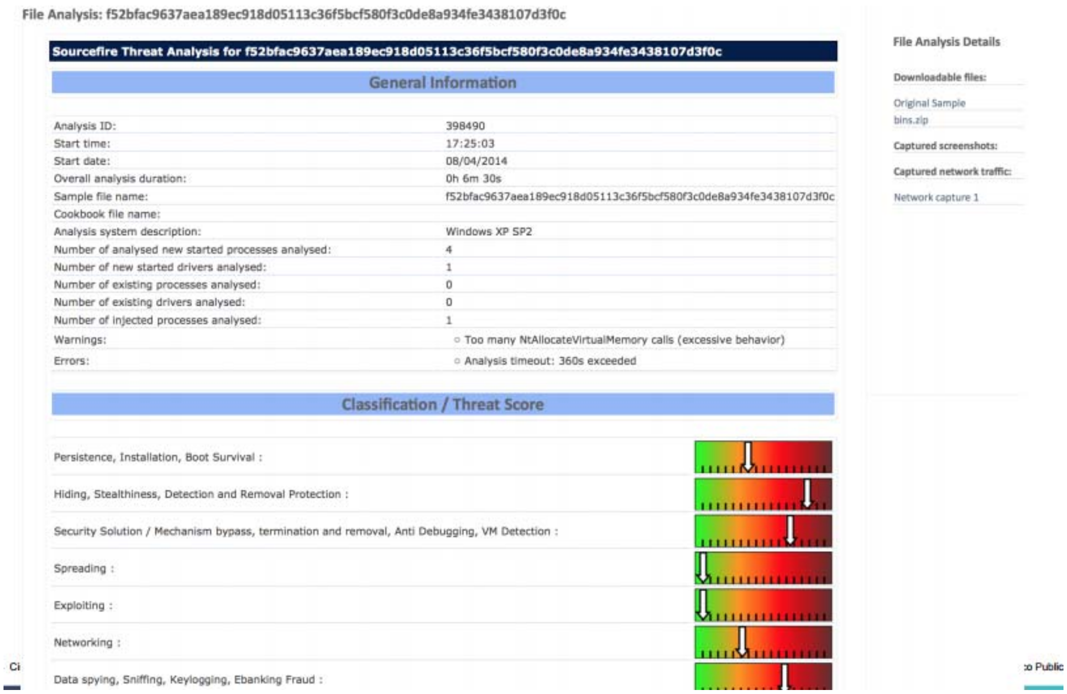
107. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

108. Defendant acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

109. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including, Cisco AMP for Endpoints, Cisco AMP for Networks, Cisco AMP for ASA with FirePOWER Services, Cisco AMP

Private Cloud Virtual Appliance, Cisco AMP for CWS, ESA, or WSA, Cisco AMP for Meraki MX, Cisco AMP Threat Grid (i.e., the Accused AMP Products), and the Accused Talos Service (collectively, the "'494 Accused Products").

110. The '494 Accused Products embody the patented invention of the '494 Patent and infringe the '494 Patent because they practice a computer-based method comprising receiving an incoming downloadable, deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable and storing the downloadable security profile data in a database. For example, Cisco AMP for Endpoint receives an incoming downloadable, and performs a lookup in the cloud where a downloadable security profile is derived and stored in a database, as shown below.



File Analysis: f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c

Sourcefire Threat Analysis for f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c

General Information

Analysis ID:	398490
Start time:	17:25:03
Start date:	08/04/2014
Overall analysis duration:	0h 6m 30s
Sample file name:	f52bfac9637aea189ec918d05113c36f5bcf580f3c0de8a934fe3438107d3f0c
Cookbook file name:	
Analysis system description:	Windows XP SP2
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Warnings:	○ Too many NtAllocateVirtualMemory calls (excessive behavior)
Errors:	○ Analysis timeout: 360s exceeded

Classification / Threat Score

Persistence, Installation, Boot Survival :

Hiding, Stealthiness, Detection and Removal Protection :

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection :

Spreading :

Exploiting :

Networking :

Data spying, Sniffing, Keylogging, Ebanking Fraud :

File Analysis Details

Downloadable files:

Original Sample

bins.zip

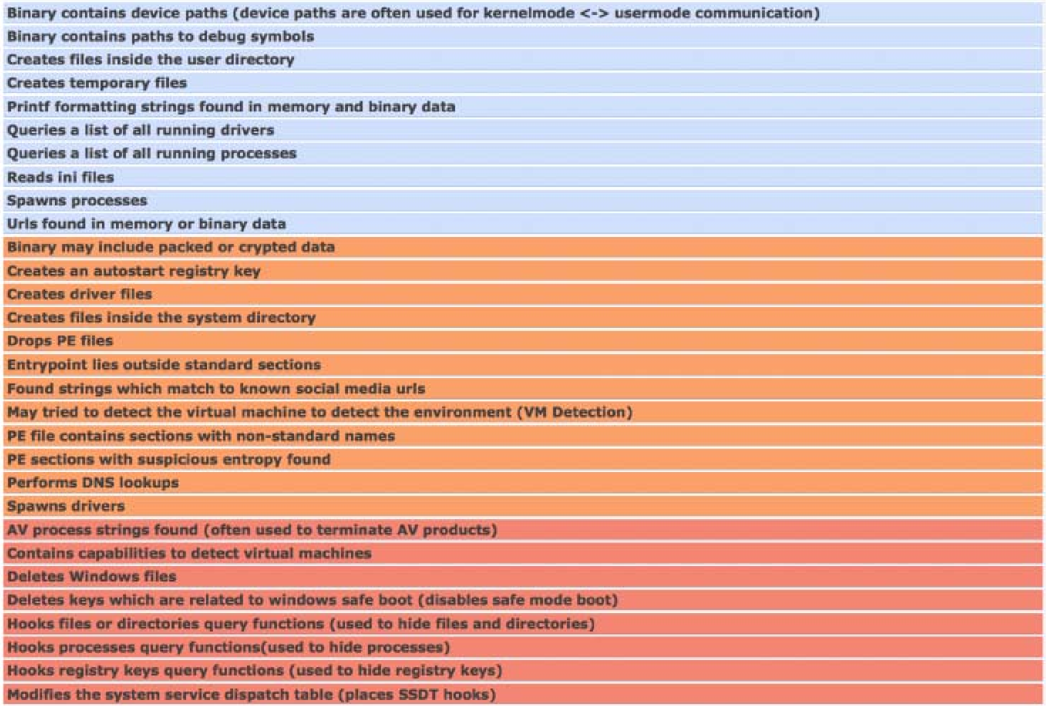
Captured screenshots:

Captured network traffic:

Network capture 1

See http://ftp.cisco.cz/Seminare/2013-ConnectClub/2014-05-28-AMP-GyorgyAcs.pdf, attached hereto as Exhibit 29.

111. As shown below, a list of suspicious computer operations is collected.



Binary contains device paths (device paths are often used for kernelmode <-> usermode communication)
Binary contains paths to debug symbols
Creates files inside the user directory
Creates temporary files
Printf formatting strings found in memory and binary data
Queries a list of all running drivers
Queries a list of all running processes
Reads ini files
Spawns processes
Urls found in memory or binary data
Binary may include packed or crypted data
Creates an autostart registry key
Creates driver files
Creates files inside the system directory
Drops PE files
Entrypoint lies outside standard sections
Found strings which match to known social media urls
May tried to detect the virtual machine to detect the environment (VM Detection)
PE file contains sections with non-standard names
PE sections with suspicious entropy found
Performs DNS lookups
Spawns drivers
AV process strings found (often used to terminate AV products)
Contains capabilities to detect virtual machines
Deletes Windows files
Deletes keys which are related to windows safe boot (disables safe mode boot)
Hooks files or directories query functions (used to hide files and directories)
Hooks processes query functions(used to hide processes)
Hooks registry keys query functions (used to hide registry keys)
Modifies the system service dispatch table (places SSDT hooks)

See http://ftp.cisco.cz/Seminare/2013-ConnectClub/2014-05-28-AMP-GyorgyAcs.pdf, attached hereto as Exhibit 29.

112. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

113. Defendant's infringement of the '494 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

114. Defendant is well aware of Finjan's patents, including the '494 Patent, and has continued its infringing activity despite this knowledge. Finjan informed Defendant of its patent portfolio and infringement on or about March 2014, and have provided representative claim charts specifically identifying how Defendant's products and services infringe Finjan's patents. Finjan attempted unsuccessfully to actively engage in good faith negotiations for over two years with Defendant regarding Finjan's patent portfolio, including having a number of in-person and telephonic meetings explaining claim element by element of Defendant's infringement.

115. Despite knowledge of Finjan's patent portfolio, being provided representative claim charts of several Finjan patents, including the '494 Patent, and engaging in technical meetings regarding infringement of Defendant's products and services, Defendant has sold and continues to sell the accused products and services in complete disregard of Finjan's patent rights. As such, Defendant has acted recklessly and continues to willfully, wantonly, and deliberately engage in acts of infringement of the '494 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT IX
(Induced Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))

116. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

117. Defendant has induced and continues to induce infringement of at least Claims 1-9 of the '494 Patent under 35 U.S.C. § 271(b).

118. In addition to directly infringing the '494 Patent, Defendant indirectly infringes the '494 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '494 Patent, where all the steps of the method claims are performed by either Defendant, its customers, purchasers, users, and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '494 Patent, including Claims 1-9.

119. Defendant knowingly and actively aided and abetted the direct infringement of the '494 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '494 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '494 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '494 Patent, specifically through the use of

Cisco's AMP, Cisco's CCSI, Talos, and AMP Threat Grid technologies, and by advertising and promoting the use of the '494 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '494 Accused Products in an infringing manner.

120. Defendant updates and maintains an HTTP site with Defendant's quick start guides, administration guides, user guides, and operating instructions which cover in depth aspects of operating Defendant's offerings. *See* http://www.cisco.com/c/en/us/support/index.html/, attached hereto as Exhibit 30; *see also* http://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-configure.html, attached hereto as Exhibit 31; http://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-configure.html/, attached hereto as Exhibit 32; http://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html, attached hereto as Exhibit 33; http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/products-configuration-examples-list.html, attached hereto as Exhibit 34; http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-configuration-examples-list.html, attached hereto as Exhibit 35; http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 36; http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html, attached hereto as Exhibit 37; https://meraki.cisco.com/support/, attached hereto as Exhibit 38; http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html, attached hereto as Exhibit 39.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendant has infringed and is infringing the '844 Patent, the '780 Patent, the '633 Patent, the '154 Patent, and the '494 Patent; has induced infringement and is inducing infringement of the '844 Patent, the '780 Patent, the '633 Patent, the '154 Patent, and the '494 Patent;

B. A preliminary and permanent injunction against Defendant and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the ‘844 Patent, the ‘780 Patent, the ‘633 Patent, the ‘154 Patent, and the ‘494 Patent, or inducing the infringement of the ‘844 Patent, the ‘780 Patent, the ‘633 Patent, the ‘154 Patent, and the ‘494 Patent and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such damages as it shall prove at trial against Defendant that is adequate to fully compensate Finjan for Defendant’s infringement of the ‘844 Patent, the ‘780 Patent, the ‘633 Patent, the ‘154 Patent, and the ‘494 Patent, said damages to be no less than a reasonable royalty;

D. A determination that Defendant’s infringement has been willful, wanton, and deliberate and that the damages against it be increased up to treble on this basis or for any other basis within the Court’s discretion;

E. A finding that this case is “exceptional” and an award to Finjan of its costs and reasonable attorneys’ fees, as provided by 35 U.S.C. § 285;

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the ‘844 Patent, the ‘780 Patent, the ‘633 Patent, the ‘154 Patent, and the ‘494 Patent; and

G. Such further and other relief as the Court may deem proper and just.

Respectfully submitted,

Dated: January 6, 2017

By: */s/ Paul J. Andre*
Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: January 6, 2017

By: *Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.